# Concealing Information in Images using Progressive Recovery

**Pooja R[1], Neha S Prasad[2], Nithya S Jois[3], Sahithya KS[4], Bhagyashri R H[5]**

*[1,2,3,4] UG Student, Department Of Computer Science and Engineering, Global Academy Of Technology, Karnataka, India.*
*[5]Assistant Professor, Department Of Computer Science and Engineering, Global Academy Of Technology, Karnataka, India.*

---------------------------------------------------------------------***---------------------------------------------------------------------

**Abstract -** *This paper proposes a method of Concealing Information in Images based on Progressive Recovery. Three parties are involved in the framework, including the content owner, the data-hider, and the recipient. The content owner selects the image and uploads it to the server. The data-hider on the server divides the image into nine channels and respectively embeds different amount of additional bits into each one to generate a stego image. On the recipient side, additional message can be extracted from the stego image, and the original image can be recovered without any errors. While most of the traditional methods use one criterion to recover the whole image and message, we propose to do the recovery by a progressive mechanism.*

***Key Words***: **Concealing data, Progressive recovery, stego image, nine channels, three criterions**

## 1. INTRODUCTION

The basic concept of hiding information in images originates from reversible data hiding (RDH) in plaintext images [1] [2]. This is profitable in the applications like cloud storage and medical systems. [3] [4]. At the cloud, when the administrator has to manage many images, he can add additional information like labels, time stamps. This provides an easier way to search images and also saves the storage overhead. When the receiver downloads the data containing additional information from the server, he/she can recover the images after decryption without any loss.

The sender encrypts an image using stream enciphering [5], and a data-hider adds additional bits into the blocks by flipping three least significant bits (LSB) in each block. On receiver side, the image is decrypted and two contender are generated by flipping again for each block. This method was further modified in [6] by attaining spatial association between neighboring blocks to have a better embedding rate, which was further improved in [7] using an embedding strategy to achieve larger embedding rate. Protected data hiding can be assured by public key modulation [8]. Hiding information can also be achieved in JPEG bit streams by lightly modifying the data [9]. One problem in [5]-[9] is that data can be extracted only after image decryption. Divisible data hiding was introduced to fix this problem, which allows one to extract data hidden directly from the encrypted image. In [10], the data-hider dissolves the pixels into sectors, and binds some LSB layers of each sector to few bits using a predefined matrix. The receiver abstracts the additional message from the marked encrypted image. After decryption, the original LSBs are regained by considering the estimated bits with the binded ones. If higher bit planes are used [11]-[13], higher embedding rate can be achieved. Some data hiding methods were also introduced to elevate embedding rates by evacuating embedding room before encryption, *e.g.*, [14] and [15]. Users with decryption key needs to view the image by decrypting the marked encrypted image. The distortion is bounded to three LBS-layers in encrypted images, as [5]-[7] and [10], to secure the decrypted image with good virtue. Overlooking to this condition, we propose a progressive recovery based divisible data hiding to accomplish a better adequacy, which is an extension to the work in [10]. We separate the embedding procedure into rounds to hide additional messages. The progressive recovery uses three criterions which is different from traditional recovery that uses only one criterion. Over progressive working, larger freight can be gained.

## 2. PROPOSED WORK

### 2.1 Problem Statement

This paper proposes a method of data hiding based on progressive recovery. Three parties are involved, the content owner, the data-hider, and the recipient. The content owner selects the original image and a symmetric key and then uploads image to the server. The data-hider divides the image and embeds additional bits to generate a stego image. On the recipient side the original image and the message hidden in image can be recovered without errors using progressive recovery.

### 2.2 Existing System

The existing system makes a connection between steganography design by minimizing embedding distortion and statistical physics. The unique aspect of this work and one that distinguishes it from prior art is that we allow the distortion function to be arbitrary, which permits us to consider spatially dependent embedding changes. The system provide a complete theoretical framework and describe practical tools, such as the thermodynamic integration for computing the rate-distortion bound and the Gibbs sampler for simulating the impact of optimal embedding schemes and constructing practical algorithms. The existing framework reduces the design of secure steganography in empirical covers to the problem of finding local potentials for the distortion function that correlate with statistical detectability in practice. The existing system presents an improved histogram-based reversible data hiding scheme based on prediction and sorting. A rhombus prediction is employed to explore the prediction for histogram-based embedding. Sorting the prediction has a good influence on increasing the embedding capacity. Characteristics of the pixel difference are used to achieve large hiding capacity while keeping low distortion. In addition, we exploit a two-stage embedding strategy to solve the problem about communicating peak points. We also present a histogram shifting technique to prevent overflow and underflow. The system we present an efficient extension of the histogram modification technique by considering the difference between adjacent pixels instead of simple pixel value. The distribution of pixel difference has a prominent maximum since image neighbor pixels are strongly correlated. Hence, there are a lot of candidates for embedding data. This observation leads us toward designs in which the embedding is done in pixel differences. Meantime, we find that sorting the prediction has much shaper histogram which would lead to significant performance improvement for histogram-based embedding. As a result, a rhombus prediction is employed in our scheme for increasing the embedding capacity. We also use a histogram shifting technique to prevent overflow and underflow. Furthermore, we use a two-stage embedding strategy to solve the problem about communicating peak points. As a result, the evaluation results show that the proposed scheme have significantly improved our previous work and derived better performance. The proposed scheme provides high capacities at small and invertible distortion. On one hand, the maximum modification to pixel values can be controlled and thus the embedding distortion can be well limited. This method can provide an embedding rate (ER) up to 0.5 bits per pixel (BPP) and it significantly out performs previous compression-based works. In particular, Tian employed a location map to record all expandable locations, and afterwards, the technique of location map is widely adopted by most RDH algorithms. Later on, work has been improved in many aspects. In, proposed a method by constructing a payload dependent location map. It has two major advantages. On the other hand, the location map used to record underflow/overflow locations is usually small in size especially for low ER case. Reversible Data Hiding methods are increasing in number as per the requirements to attain an Optimal state, In this survey it is found that according to some predefined rules the data is embedded in the Original Image or host image by choosing an optimal value. This method is an iterative method based on the size of Host image and data the optimal value is calculated using value modification under a payload distortion criterion method and moreover practical Reversible Data Hiding is obtained. In this procedure host image is divided into subset of small size images and the differences between the sub images are calculated wherever the value of difference is less the data is embedded and recovery is done in the reverse process. Histogram Shifting is recommended as one of the most important technique in the area of Reversible Data Hiding where the best results can be obtained. In this survey the author describes the overview of recent techniques involving Data Hiding using Histogram Shifting where the concentration is done on the improvement of image quality and also to increase the payload capacity in the host image. Moreover the PSNR is also has been considered to improve over the existing techniques.

**Disadvantages:**

- ➢ It cannot outperform the recently proposed schemes with additive distortion functions.
- ➢ It is also unclear how to adjust the existing additive schemes so that Gibbs construction could be applicable on them.
- ➢ It may not be immediately applicable in a non-additive case.
- ➢ It may not deviate steganalytic statistics.

- It may not be easy for an adversary to estimate the accurate costs from the stegno image

## 2.2 Proposed System

The proposed system is illustrated in Figure 1, including three parties: the content owner, the data-hider, and the recipient. The content owner selects the image and uploads the image onto a remote server. The data-hider divides the image into three sets and embeds message into each set to generate a stego image. The recipient extracts message and the original image can be losslessly recovered by progressive recovery.

In the system we have designed content owner and data hider on the same side while recipient is on the different side. Initially both content owner and recipient i.e., sender and receiver should register themselves giving their details. Later they can login and use the application as either sender or receiver as required.

The sender will select an image that is used to hide the secret message that is to be transmitted to the receiver. Sender will also select a symmetric key that is used by both sender and receiver for encryption and decryption respectively. Sender will send the selected image to the data hider for further processing. Data hider will enter the secret message that has to be embedded into the image. Data hider processes the image, segments the image, removes the distortion present in the image and then embed the message into the image to produce a stego image. This image is sent to the receiver using IP address and the port number of the receiver.

The receiver enters the symmetric key and receives the image sent by the data hider. Receiver decodes the image to get the secret message hidden in the image received. The quality of the image is retained and the message is decoded in very less time improving time efficiency thereby improving the performance of the application.

### Advantages:

- It is not necessary to assign costs simultaneously.
- Increasing a pixel value and decreasing a pixel value do not necessarily have the same cost.
- It will also be helpful in the non-additive case.
- Clustering embedding modifications in the neighborhood of unpredictable pixels should be beneficial to enhance the security of non-additive steganography as well.
- It achieves better statistical undetectability against the state-of-the-art steganalyzers

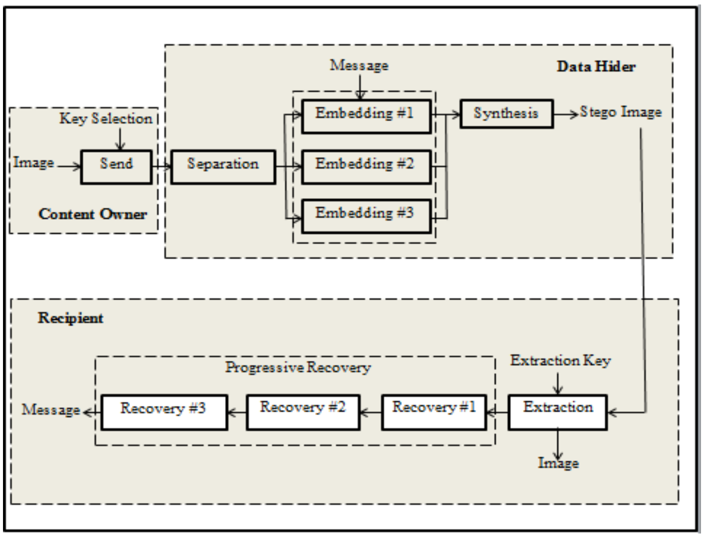


Figure 1: Framework of Proposed System

## 3. RESULT

Below are the snapshots of the application for system designed which illustrates the working of the system more effectively.

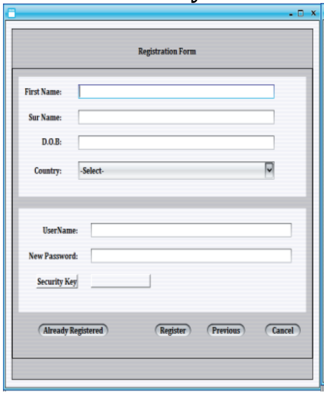
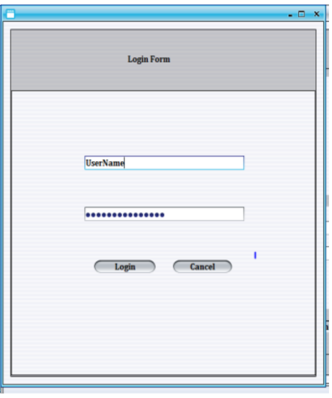


Figure 2: Registration Form



UserName
•••••••••••••••

Figure 3: Login Form

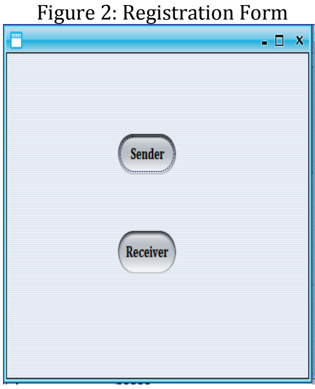
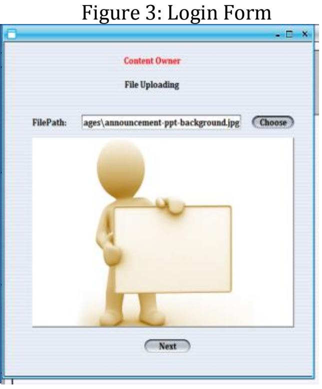
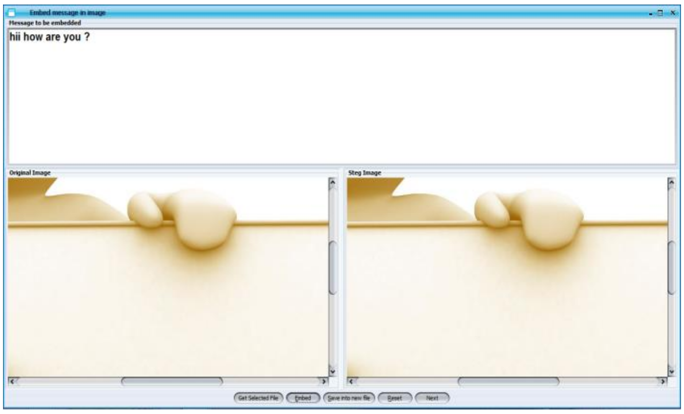


Figure 4: Main Page



FilePath: ages\announcement-ppt-background.jpg

Figure 5: Content Owner uploads File



Message to be embedded: hii how are you ?

Figure 6: Data Hider inputs the message to be embedded

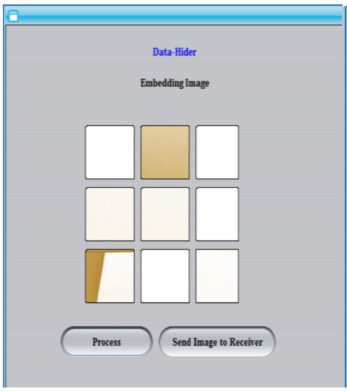
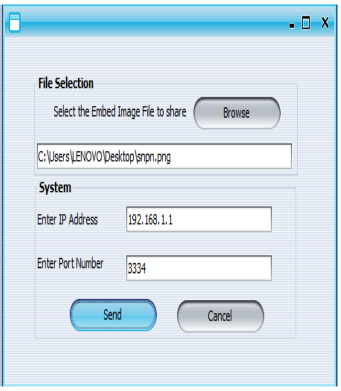


Figure 7: Data Hider Embedding text in image fragments

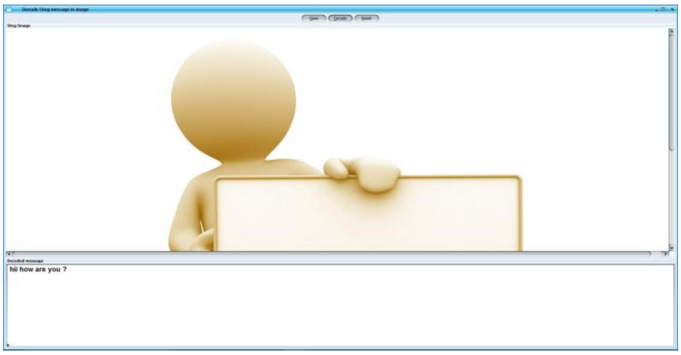


Select the Embed Image File to share: C:\Users\LENOVO\Desktop\snpn.png

Enter IP Address: 192.168.1.1

Enter Port Number: 3334

Figure 8: Data Hider sends Image using IP address



Decoded message: hii how are you ?

Figure 9: Receiver receives Image and decodes it to get the text embedded in it

## 4. CONCLUSION

Finally, a new protocol to disguise data in any digital media for three parties is proposed in this paper. Main improvement is extending the traditional recovery to the progressive based recovery. The progressive recovery based data hiding provides a better prediction way for estimating the LSB-layers of the original image using three rounds. Since Data hiding is equivalent to a rate-distortion problem, capability of the method should be evaluated by both the distortion and the embedding rate. For achieving better embedding rate, this paper limits the distortion to three LSB-layers.

## 5. FUTURE SCOPE

Database of users has been stored on Content owner's Server. Instead, the database can be maintained in cloud for better performance. Multiple owners can be made to send information to multiple receivers simultaneously without affecting the network traffic. Multiple media files can be used like video, audio etc instead of just image file to embed the text. Audio, video, image messages can also be made to embed within some media files for better efficiency. Embedding rate can be improved by considering fewer LSB layers.

## REFERENCES

[1] X. Hu, W. Zhang, X. Li, and N. Yu, Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding, *IEEE Transactions on Information Forensics and Security*, 10(3): 653-664, 2015

[2] X. Li, W. Zhang, B. Ou, and B. Yang. A brief review on reversible data hiding: current techniques and future prospects, *IEEE China Summit & International Conference on Signal and Information Processing (ChinaSIP)*, 426-430, 2014

[3] H. Wang, W. Zhang, and N. Yu, Protecting Patient Confidential Information based on ECG Reversible data hiding, *Multimedia Tools and Applications*, doi:10.1007/s11042-015-2706-2,2015

[4] Z. Fu, X. Sun, Q. Liu, et al. Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing, *IEICE Transactions on Communications*, 98(1): 190-200, 2015

[5] X. Zhang, Reversible data hiding in encrypted images, *IEEE Signal Processing Letters*, 18(4): 255–258, 2011

[6] W. Hong, T. Chen, and H. Wu, An improved reversible data hiding in encrypted images using side match, *IEEE Signal Processing Letters*, 19(4): 199–202, 2012

[7] M. Li, D. Xiao, A. Kulsoom, and Y. Zhang, Improved reversible data hiding for encrypted images using full embedding strategy, *Electronic Letters*, 51(9): 690-691, 2015

[8] J. Zhou, W. Sun, L. Dong, et al. Secure reversible image data hiding over encrypted domain via key modulation, *IEEE Transactions on Circuits and Systems for Video Technology*, 26(3): 441-452, 2016

[9] Z. Qian, X. Zhang, and S. Wang, Reversible data hiding in encrypted JPEG bitstream, *IEEE Transactions on Multimedia*, 16(5): 1486-1491, 2014

[10] X. Zhang, Separable reversible data hiding in encrypted image, *IEEE Transactions Information Forensics and Security*, 7(2): 826–832, 2012

[11] Wu X, Sun W. High-capacity reversible data hiding in encrypted images by prediction error, *Signal processing*, 104: 387-400, 2014

[12] Z. Qian, and X. Zhang, Reversible data hiding in encrypted image by distributed encoding, *IEEE Transactions on Circuits and Systems for Video Technology*, 26(4): 636-646, 2016

[13] X. Zhang, Z. Qian, G. Feng and Y. Ren, Efficient reversible data hiding in encrypted images, *Journal of Visual Communication and Image Representation*, 25(2): 322-328, 2014

[14] K. Ma, W. Zhang, et al. Reversible data hiding in encrypted images by reserving room before encryption, *IEEE Transactions Information Forensics and Security*, 8(3): 553-562, 2013

[15] X. Cao, L. Du, X. Wei, et al. High capacity reversible data hiding in encrypted images by patch-level sparse representation, *IEEE Transactions on Cybernetics*, 46(5): 1132-1143, 2016